ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 8, August 2015

Improved Secure Database Service and Management System against SQL Injection Attacks

M.Rajashree and S.Syed Ibrahim

Research Scholar, PG and Research Department of Computer Science, Jamal Mohamed College, Trichy, India.
Assistant Professor, PG and Research Department of Computer Science, Jamal Mohamed College, Trichy, India

Abstract: The Database as a Service (DBaaS) is a novel paradigm through which cloud providers offers the possibility of storing data in remote databases. The main concerns that are preventing the diffusion of DBaaS are related to data security and confidentiality issues. Hence, the main alternative seems the use of cryptography, which is an already adopted solution for files stored in the cloud, but that represents an open issue for database operations over encrypted data. In this paper, we propose a cloud database architecture based framework that encapsulate data through different layers of encryption. This adaptive architecture is attractive because it does not require to define at design time which operations are allowed on each column, and because it can guarantee at runtime the maximum level of data confidentiality for different SQL operations. Unfortunately, this scheme is affected by high computational costs. So we implement this framework in multimedia data files. However, through a prototype implementation of an encrypted cloud database, we show that adaptive framework can be well applied to a cloud database paradigm, because most performance overheads are masked by network latencies. We demonstrate through a large set of experiments that these encryption schemes represent a feasible solution for achieving data confidentiality in public cloud databases, even from a performance point of view.

Keywords: Database as a service, Encryption schemes, Encrypted cloud database, SQL operations

I. INTRODUCTION

The aim of system is, to integrate cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data. We use cloud for uploading owner's data. Data Owner who has uploaded his data on cloud he is not ensure about his data, so we have to store his data on the cloud by encrypting his data. This encryption of data takes place at client side and metadata of that data also created i.e. secureDBaaS concept. This encrypted data is stored at the cloud along with its encrypted metadata. Then the authorized clients can access the data by using only metadata. This is the first solution supporting geographically distributed clients to connect directly to an encrypted cloud database, and to execute concurrent and independent operations including those modifying the database structure. The proposed system has the further advantage of eliminating intermediate proxies that limit the elasticity, availability, and scalability properties that are intrinsic in cloud-based solutions. SecureDBaaS provides several original features that differentiate it from previous work in the field of security for remote database services as in figure 1.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 8, August 2015

Figure 1: Cloud Database as a service

II. RELATED WORK

In previous research papers, they are tried to improve the independent Access method in outsourced storage in cloud. They are focusing to improve the reliability of communication .we doesn't focus any illegal interaction compensation. A.J. Feldman [3] describes SPORC's framework and protocols for real-time collaboration. SPORC provides security and privacy against both an un-trusted server that mediates communication and other clients that lack access control permissions and demonstrate how to support dynamic access control, which is challenging because SPORC supports concurrent operations and offline editing. P. Mahajan [5] analyze Depot is that cloud storage service providers (SSPs), such as S3 and Azure, are fault-prone black boxes operated by a party other than the data owner. Indeed, clouds can experience software bugs, correlated manufacturing defects, misconfigured servers and operator error, malicious insiders, bankruptcy, undiagnosed problems. R.A. Popa [8] proposes CryptDB which can exploit software vulnerabilities to gain unauthorized access to servers curious or malicious administrators at a hosting or application provider can snoop on private data and attackers with physical access to servers can access all data on disk and in memory. V. Ganapathy [13] generates privacy constraints over it randomly with properties and then generates as many privacy constraints as the number of attributes in the relation. Privacy constraints vary in size from one to the number of attributes in the relation. The attributes that are part of each constraint are selected at random from the available attributes without replacement.

III. ENCRYPTED CLOUD FILES DATABASE

With cloud research technology, there were plenty of important policy issues may include like privacy, secrecy, anonymity, government surveillance, stability etc., Of these entire most crucial one will be security, through which how the cloud provider assures. Generally cloud computing features different class of customers that features academicians, everyday users and also enterprises etc., in which in turn their motivation is always to move about the cloud regarding deploying software, managing assets etc. Existing system implement a significant security improvement to the using novel architecture that integrates cloud database services with data confidentially and the possibility of executing the concurrent operation on encrypted data. This is the first solution supporting geographically distributed clients to connect directly to an encrypted cloud database and to execute concurrent and independent operation including those modifying the database structure. Secure DBaaS provides several original features that differentiate it from previous work in the field of security for remote database services. This architecture does not require modifications to the cloud database and it is immediately applicable to existing cloud DBaaS.

IV. CONCURRENT ENCRYPTED MULTIMEDIA CLOUD DATABASE

We propose SecureDBaaS as the first solution that allows cloud tenants to take full advantage of DBaaS qualities, such as availability, reliability, and elastic scalability, without exposing unencrypted data to the cloud provider. The architecture design was motivated by goal: to allow multiple, independent, and geographically distributed clients to execute concurrent operations on encrypted

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 8, August 2015

data, including SQL statements that modify the database structure. We can perform meta data management that includes all files such as text files, document files and multimedia files. Metadata generated by SecureDBaaS contain all the information that is necessary to manage SQL statements over the encrypted database in a way transparent to the user. Metadata management strategies represent an original idea because SecureDBaaS is the first architecture storing all metadata in the untrusted cloud database together with the encrypted tenant data.

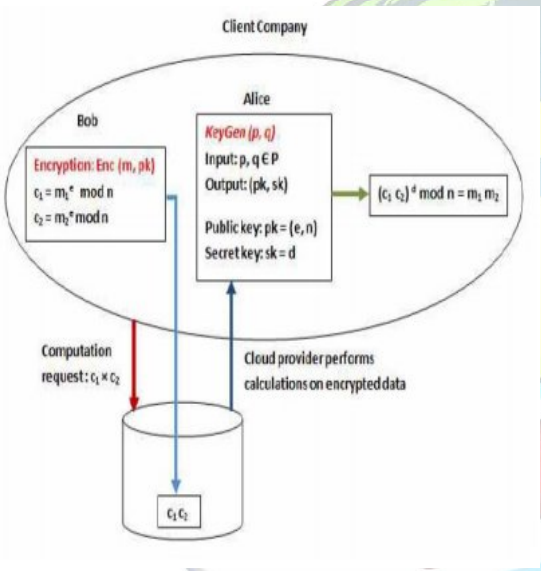


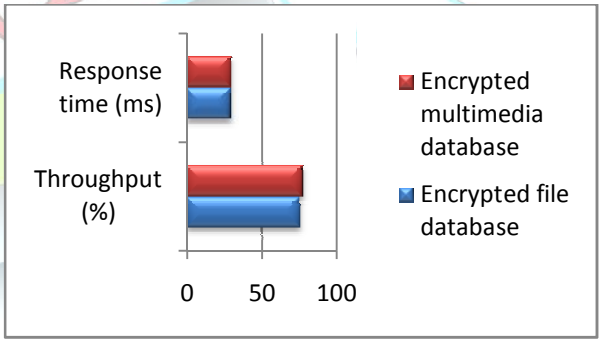
Fig 2: Proposed process

V. EXPERIMENTAL RESULTS

This paper explains encrypted databases. The upload files and multimedia data using keys, to maintain the privacy of outsourced data in a secure manner. Independent Access between Cloud and data owner. The owner is capable of not only archiving and accessing the data stored by the cloud service provider, but also updating and scaling this data on the remote servers. We can measure this performance using throughput and response time. Our proposed system maintains same time and throughput at the time of multimedia analysis. The following table shows the performance of the system in experimental manner.

Network delay	SQL commands	Plain text response time(ms)	Encrypted response time(ms)	Throughput (%)
LAN	Select	0.35	0.65	78
	Update	0.28	0.63	80
	Delete	0.27	0.612	85
	Insert	0.32	0.59	87
20 ms	Select	10.45	10.23	65
	Update	10.54	10.43	63
	Delete	10.65	10.32	62
	Insert	10.54	11.54	60
80 ms	Select	40.65	40.57	54
	Update	40.32	40.12	58
	Delete	40.43	40.67	62
	Insert	40.78	41.32	64

And shows the performance of the system in graphical manner as follows



VI. CONCLUSION

Cloud database services are integrated with data confidentiality and concurrent access models. Secure database as a service (SecureDBaaS) Framework is used to manage data access in encrypted cloud databases. The SecureDBaaS

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 8, August 2015

scheme is enhanced with data integrity features. Concurrent database structure modification and query security tasks are improved with security methods. The system eliminates the intermediate proxies in database management process. Database structure modification mechanism is adopted for multi user environment. The system improves the availability and scalability features. We propose associate innovative design that guarantees confidentiality of knowledge keeps publicly cloud databases. The proposed part of the analysis includes solutions to support synchronous SQL operations (including statements modifying the information structure) on encrypted information issued by heterogeneous and presumably geographically spread shoppers. The response time in query processing is reduced by the system. Clients are capable of reading and writing data on cloud database, and each client has limited access as per his\her designation for organizations security purpose. Further work is, we can try and improve the SQL aware encryption techniques.

REFERENCES

[1]. M. Armbrust et al., "A View of Cloud Computing," Comm. of the ACM, vol. 53, no. 4, pp. 50-58, 2010.

[2]. W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," Technical Report Special Publication 800-144, NIST, 2011.

[3]. A.J. Feldman, W.P. Zeller, M.J. Freedman, and E.W. Felten, "SPORC: Group Collaboration Using Untrusted Cloud Resources," Proc. Ninth USENIX Conf. Operating Systems Design and Implementation, Oct. 2010.

[4]. J. Li, M. Krohn, D. Mazie`res, and D. Shasha, "Secure Untrusted Data Repository (SUNDR)," Proc. Sixth USENIX Conf. Opearting Systems Design and Implementation, Oct. 2004.

[5]. P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish, "Depot: Cloud Storage with Minimal Trust," ACM Trans. Computer Systems, vol. 29, no. 4, article 12, 2011.

[6]. H. Hacigu¨mu¨ s¸, B. Iyer, and S. Mehrotra, "Providing Database as a Service," Proc. 18th IEEE Int'l Conf. Data Eng., Feb. 2002.

[7]. C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," Proc. 41st Ann. ACM Symp. Theory of Computing, May 2009.

[8]. R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting Confidentiality with Encrypted Query Processing," Proc. 23rd ACM Symp. Operating Systems Principles, Oct. 2011.

[9]. H. Hacigu¨mu¨ s¸, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model," Proc. ACM SIGMOD Int'l Conf. Management Data, June 2002.

[10]. V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R. Motwani, "Distributing Data for Secure Database Services," Proc. Fourth ACM Int'l Workshop Privacy and Anonymity in the Information Soc., Mar. 2011.